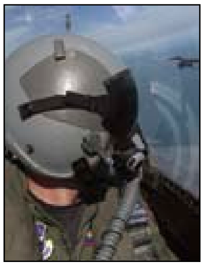
CWID 2006 DEMONSTRATION

Guidebook Contents

Published May 2006
PUBLISHED BY: Lt. Col. Beatriz Westmoreland, USAF, CWID Director
EDITOR: Michael Brown, Chief, Public Relations and Protocol, CWID JMO
Creative Director: Joan Strong, CWID JMO
For information or to obtain copies, contact: CWIDPA@langley.af.mil
www.cwid.js.mil

NOTES



CWID 2006 DEMONSTRATION

Executive Summary

The Coalition Warrior Interoperability Demonstration (CWID) is a Chairman of the Joint Chiefs of Staff annual event that features Interoperability Trials (ITs) focused on selected core objectives defined by combatant commanders. ITs that are approved for participation are required to provide a new capability or to improve on an existing capability in support of the prioritized objectives.

The demonstration tests and evaluates technologies and capabilities for exchanging information among agencies, services and this year's host combatant commander, U.S. European Command (USEUCOM). CWID enables U.S. combatant commands and the international community to investigate command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) solutions that focus on relevant and timely objectives for enhancing coalition interoperability. The coalition interoperability effort seeks solutions that can be applied in the operational community and enables a standard procedure for information sharing between coalition partners.

OBJECTIVES

- COALITION COMMAND AND CONTROL (C2)
- COALITION INFORMATION SHARING
- INTEGRATED LOGISTICS
- CONTINUITY OF OPERATIONS
- NET-CENTRIC ENTERPRISE SEVICES

CWID offers a challenging scenario that examines trial capabilities. The scenario has two parts: one for the Combined Task Force (CTF) and one for Homeland Security and Homeland Defense (HLS/HLD). For the CTF portion, CWID provides a framework that facilitates participation of ITs through a full range of military operations conducted by U.S. and coalition forces. CTF operations are set in a notional context in fictitious countries. For the HLS/HLD portion of the scenario, federal, state and local agencies respond to terrorist attacks within the U.S. These fictitious attacks are tied to the conventional U.S. led CTF operations on another continent.

U.S. Joint Forces Command (USJFCOM), Norfolk, Va., is responsible for planning and execution oversight of CWID. The command targets information technologies that can be moved into operational use within 18 months of the execution period.

The Defense Information Systems Agency (DISA), Arlington, Va., manages day-to-day program operations, directs the demonstration's execution and engineers the demonstration network. The demonstration runs over the Combined Federated Battle Laboratories Network (CFBLNet) classified network and the DISN-LES unclassified network. The events-driven network has an architecture that enables controlled and protected communications as prescribed by operational requiremen and national security policies.

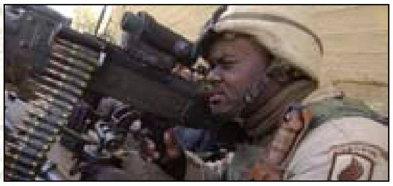
Find visitor procedural details for each site at the guidebook U.S. Sites & Agencies tab and the Coalition Partners tab.

U.S. Northern Command (USNORTHCOM), Colorado Springs, Colo., manages the HLS/HLD portion of the demonstration. The command uses CWID as a proving ground for emerging technology application through the entire spectrum of first responders.

CWID is scheduled for execution and technology assessment 12-22 June 2006, with a set-up week 5-9 June. Assessments will be published in a formal report later in 2006.

The host site is USEUCOM, Kelley Barracks, Stuttgart, Germany, but visitors can experience operations and interoperability trials worldwide. Other U.S. visitor sites include: HLS/HLD in Colorado Springs, Colo.; the U.S. Army, U.S. Marine Corps and National Guard Bureau at Naval Surface Warfare Center, Dahlgren Division, Va.; the U.S. Navy at SPAWAR, San Diego, Calif.; and the U.S. Air Force at Electronic Systems Center, Hanscom AFB, Mass.

The global network includes Australia, Canada, New Zealand, United Kingdom, and many NATO nations, also with demonstration sites and visitor access. There are more than 20 international participants at more than 25 sites around the world.



HISTORY OF THE DEMONSTRATION

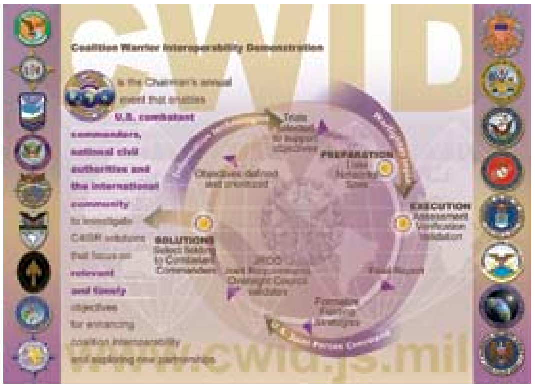
From Concept to Frontline

CWID traces more than 16 years of history to the establishment of the Secure Tactical Data Network (STDN) series originated by the U.S. Army to demonstrate emerging command, control, communications and computer (C4) capabilities.

STDN 1 and 2 concentrated on Army-only issues while STDN 3 brought the first multi-service participation. The Joint Staff recognized that advances in communications and information technology in the public sector were outpacing Department of Defense capabilities.

In 1993, the Joint Staff assumed sponsorship of the STDN series under the C4I for the Warrior concept. Using the Defense Information Systems Agency (DISA) as the Executive Agent, the Joint Staff directed DISA, in concert with a lead Service, to organize network experiments to bring emerging public sector, and other government agency technologies, into DoD projects and into the warfighters' sphere of recognition. DISA was also directed to improve joint C4 interoperability.

In 1994, the annual STDN efforts evolved into the first Joint Warrior Interoperability Demonstration (JWID). The Air Force was the lead service and U.S. Atlantic Command was the host combatant command. The idea of moving from a static, one-dimensional picture of the battlefield to a near real-time, multi-dimensional battlespace picture became reality to joint and combined warriors. Key efforts in JWID '94 included the demonstration of baseline segments of what became the Global Command and Control System (GCCS). Six weeks after the conclusion of JWID '94, GCCS was operationally deployed to U.S. Atlantic Command to support military operations in Haiti. Full operational deployment of GCCS to all combatant commanders occurred within 12 months after JWID '94.


CWID
Coalition Warrior Interoperability Demonstration
is the Chairman's annual event that enables
U.S. combatant commanders, national civil authorities and the international community
to investigate C4ISR solutions that focus on
relevant and timely
objectives for enhancing coalition interoperability and exploring new partnerships
Objectives defined and prioritized
PREPARATION
EXECUTION
Assessment
Verification
Validation
SOLUTIONS
Select fielding to Combatant Commanders
JROC Joint Requirements Oversight Council validation
Final Report
Formalize Fielding Strategies
www.cwid.js.mil

In 1997, the Chairman of the Joint Chiefs of Staff mandated interoperability in Joint Vision 2010, envisioning future conflicts as coalition operations. JWID assisted in this development through establishing itself as a coalition interoperability forum through invitations to the Combined Communications Electronics Board

THEN & NOW

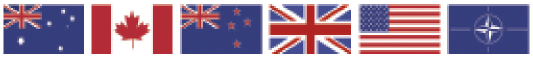
Identifying technologies for the joint and coalition warfighter...

CWID 2005

U.S.NORTHERN COMMAND

- ■ Multi-level-secure Information Infrastructure (MI2), implementing Secure Network Server (SNS) from 2004, addresses information sharing and information assurance between civil and government agency first responders
- ■ Advanced Geospatial Imagery Library Enterprise (AGILE), NGA-sponsored technology in operational use
- ■ Pliable Display Technology (PDT) in operational use; AGILE output device
- ■ Request for Information WebTool (RFI) in operational use, Canadian Forces; being considered for NGA National System for Geospatial-Intelligence (NSG) baseline
- ■ Masking Shunt undergoing further research and target funding
- ■ Weapons of Mass Destruction Common Operational Picture (WMD COP) in use at USNORTHCOM Operations Center; deployed to support DHS hurricane relief, Louisiana and Mississippi
- ■ Tactical Medical Coordinating System (TacMedCS) undergoing refinement and field trials with U.S. Marine Corps
- ■ Joint Warning And Reporting Network (JWARN) continuing integration into current systems
- ■ Marine Air Ground Task Force Continuity of Operations System (MAGTFCS) supporting U.S. Marine Corps field operations
- ■ Incident Commanders' Radio Interface (ICRI) purchased by Joint Task Force-Civil Support

(CCEB) nations (Australia, Canada, New Zealand and the United Kingdom) and NATO beginning with JWID '94 and continuing to the present. While these invited participants use JWID to perform their own technology demonstrations and joint interoperability trials, their main intent is to promote and ensure C4 interoperability with the U.S.



EXPANSION

In 1998, JWID evolved into a two-year process to pursue selection and limited fielding of C4 technologies to the warfighting combatant commanders. The Theme (first) Year conducted demonstrations and interoperability trials and selected "Gold Nuggets" for support and continued improvement during the Exploitation (second) Year, with eventual fielding to combatant commands. JWID '98 fielded three Gold Nuggets to warfighters, selected from results of JWID '97.

Due to U.S. Y2K concerns, JWID '99-R was revised to focus upon coalition interoperability trials between the U.S. and CCEB/NATO nations. To more easily promote such trials and other C4I experiments, the Coalition Wide Area Network (CWAN) established annually for JWID evolved into the standing Combined Federated Battle Laboratories Network (CFBLNet). This flexible network permits C4I experimentation among the U.S. and nations of CCEB/NATO, on a year-round basis, using systems jointly owned and managed by CFBL membership.

JWID '00-'01 restored the two-year cycle, with 23 U.S. demonstrations and 145 combined/coalition demonstrations at multiple, worldwide sites. Two Gold Nuggets were fielded in 2001. In addition, a Distributed Collaborative Tool Set (DCTS, now Defense Collaboration Tool Suite) was refined and subsequently selected for worldwide fielding to the Unified Commands. JWID '01 DCTS trial execution and assessment permitted DISA to field the capability, within 72 hours, in support of OSD requirements following the terrorist attacks of September 11th , to multiple DoD networks.

COALITION INTEROPERABILITY

JWID 2002 featured transition from a limited fielding of technology to a full focus on coalition interoperability, led by U.S. Pacific Command (USPACOM), the host combatant commander. The demonstration included Pacific Rim nations in a Pacific Theater Initiative (PTI), with Japan, South Korea, Singapore, and Thailand participating while Malaysia and the Philippines observed operations. Multiple coalition partners were integrated on the Multinational Task Force (MTF) and component staffs to maximize opportunities. In addition, the JWID CWAN continued use of CFBLNet architecture and services established

(JTF-CS); purchased and in use by DHS agencies, National Interagency Fire Center, Louisiana Army NationalGuard, fire departments, mining operations, sheriff and police departments in support of disaster relief

- ARINC Wireless Interoperability Network Solution (AWINS) deployed with National Guard in support of hurricane relief efforts
- Multi-Level Chat (ML Chat) and One Way File Transfer (OWFiT) under development for U.S. Central Command (USCENTCOM) area of operations
- Global Broadcasting System (GBS) fielded for joint military exercise and undergoing evaluation for integration with current operational systems
- Commercial Joint Mapping Tool Kit (C/JMTK) is a continuing NGA program planned as basis for participation in Network-Centric Capabilities Pilot (NCCP)

2004

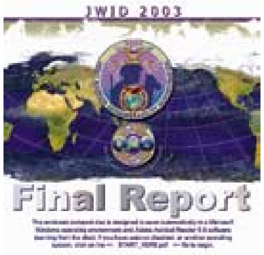
U.S.NORTHERN COMMAND

- Joint Protection Enterprise Network (JPEN), U.S. Northern Command (USNORTHCOM) and U.S. Air Staff working to support development
- Area Security Operations Command and Control (ASOCC) fielded in support of U.S. Army with Departments of Homeland Security (DHS), Justice (DoJ) and Defense (DoD)
- Rapid Response System-Deployable (RRS-D) fielded with U.S. Marine Corps in support of federal and civil response to Hurricanes Katrina and Rita
- PKI Interop undergoing review, fielded for USPACOM U.S. Navy tactical messaging exercise in a coalition environment
- Critical Infrastructure Protection Dismounted Data Automated Communication Terminal (D/DACT) wireless communication nodes; National Guard considering for first responder and anti-terror operations
- Information Relevance Prototype (IRP) in further development with NGA
- Palenterra provides geospatial situational awareness for HLS; in use by NGA

2003

U.S. MARINE CORPS & U.S. PACIFIC COMMAND

- Bi-Directional Korean MachineTranslation Tool Suite fielded with U.S.Army, U.S. Forces Korea (Phrasalator)
- Blue Force Tracking in use as component of command and control suite
- Coalition Warfare Program (CWP)
- PKI Express evolved into PKI Interop, 2004, enabling root network certification for mulitple levels of security



in past demonstrations. U.S. Joint Forces Command (USJFCOM) fielded a JWID demonstrated language translation device following JWID 2002.

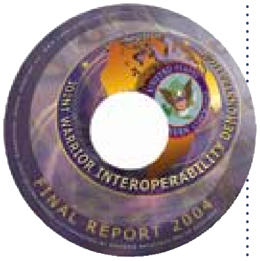
JWID 2003 took coalition interoperability to new heights. USPACOM guided the CTF and, for the first time, Japan, South Korea, Thailand and Singapore provided staffing to expand information exchange over dual domains. One key focus for 2003 included management of information exchange between the traditional 6-eyes network to a larger, more robust 10-eyes network. The larger network was vital to JWID's success because Pacific Rim nations needed effective information to serve in MTF staff positions. JWID 2003 addressed multi-level security technical solutions and refinement of coalition policies and procedures to overcome issues surrounding information exchange requirements.

Defense Information Systems Agency (DISA) assumed duties as the lead agency, providing broad-base management support of JWID activities. Four Coalition Interoperability Trials (CITs) with especially noteworthy performance were submitted to USJFCOM J861, for consideration for limited fielding as part of the new J861 Transformation Change Package (TCP) fielding process.

HOMELAND SECURITY

JWID 2004 featured U.S. Northern Command (USNORTHCOM) as the Host Combatant Commander. USNORTHCOM brought a Homeland Security/Homeland Defense focus to the demonstration. This approach broke new ground beyond the traditional JWID coalition interoperability area, adding government interagency information sharing. USNORTHCOM, in a departure from previous JWIDs, invited agencies within the Department of Homeland Security, including first-time participation for the Federal Emergency Management Agency (FEMA), the Federal Bureau of Investigation (FBI), the U.S. Coast Guard, and the National Guard Bureau. Limited coalition participation between these organizations occurred as Canada's Office of Critical Infrastructure Protection joined in the interoperability trials. This activity offers significant potential for more extensive cooperation between other coalition homeland security organizations and their U.S. counterparts. U.S. Joint Forces Command (USJFCOM) filled an ancillary role, assisting with select fielding of technologies to combatant commanders. JWID 2004 involved 25 countries, military services, and government agencies participating in a scripted scenario over a global network.

2004•2005
UNITED STATES NORTHERN COMMAND
JOINT WARRIOR INTEROPERABILITY DEMONSTRATION



USNORTHCOM was host Combatant Commander in 2005 as the demonstration moved forward with a name change. Now the Coalition Warrior Interoperability Demonstra-

- ■ Artillery Systems Cooperation Activity (ASCA) Spanish targeting system; interoperable with Army and Marine Corps targeting systems
- ■ Expand Network Accelerators fielded with U.S. Navy and allied naval forces for low-speed data transmission links
- ■ First multi-domain coalition network

2002
U.S. MARINE CORPS & U.S. PACIFIC COMMAND

- ■ Naval Fire Control System (NFCS) provides automatic gun plots; Army and Marine Corps deploying on combatant and amphibious ships
- ■ Comprehensive Assessment Methodology implemented
- ■ Established multinational Coalition Vulnerability Analysis Team (CVAT) developed with Concept of Operations (CONOPS) documentation
- ■ Language Translation Services in instant message format devices procured for combatant commands
- ■ Pacific Rim nations involved with U.S. Pacific Command sponsorship

2000-2001
U.S. AIR FORCE & U.S. SPACE COMMAND

- ■ Defense Collaborative Tool Suite(DCTS) deployed to Afghanistan for Operation Enduring Freedom; subsequently designated DoD standard tool set
- ■ Coalition Portal for Imagery and Geospatial Services (CPIGS) providing operational geospatial intelligence support to U.S. Army Airbornen Dragon Eye Unpiloted Aerial Vehicle(UAV) sponsored by Marine Corps Warfighting Lab; being considered for Army, National Guard and Coast Guardwarfighters and first responders
- ■ Defense Message System (DMS)
- ■ Silent Runner® deployed to three combatant commands
- ■ PATROL© deployed to eight combatant commands
- ■ GCCS first COP exchange with Allied nations
- ■ Direct support from National Geospatial-Intelligence Agency (NGA)

1999-Revised
U.S. AIR FORCE & U.S. JOINT FORCES COMMAND

- ■ CCEB and NATO nations demonstrate over U.S. Combined Wide AreaNetwork (CWAN)
- ■ CWAN transitions to Combined Federated Battle Lab Network (CFBLNet) for year-round Coalition testing
- ■ COP Interface eXchange (CIX)
- ■ eXtensible Markup Language (XML) viewing of Air Tasking Order (ATO)

2005
COALITION WARRIOR INTEROPERABILITY DEMONSTRATION
UNITED STATES NORTHERN COMMAND

tion (CWID), the shift from "Joint" to "Coalition" describes the larger community of participants, including national and international government agencies. A new name was not the only change for CWID in 2005.

USJFCOM formally assumed oversight for planning and execution of CWID 2005 from the Joint Staff in July 2004. This involvement brings USJFCOM advocacy for U.S. combatant command interoperability shortfall resolution to the forefront. USJFCOM's objectives include (1) to ensure CWID demonstrates relevant technologies that address combatant commander capability gaps, (2) to investigate military, coalition and interoperability solutions and (3) to identify technologies suitable for prototype initiatives.

CWID 2005 featured revitalization of the planning and collaboration web site, including readily accessible general information. Online trial submission abbreviated initial proposal processes for interested technology representatives. Additionally, CWID established a Concept of Operations (CONOPs) for all recurring aspects of the planning and execution process.

The CWID 2005 Execution results were noteworthy in that most ITs successfully achieved their stated objectives. More than 400 operators from the military and supporting agencies, at multiple U.S. and coalition sites, executed the scenario events to evaluate and report on trial performance.

Fifteen trials were considered "success stories," moving forward for continued development. Seven ITs were selected for Service, Agency, or limited Combatant Commander fielding (including fielding in support of Hurricane Katrina). Two ITs achieved milestones and continue spiral development as Programs of Record. One was selected for funding via a Congressional Plus-up for further research and development, and one was submitted as a Limited Acquisition Authority candidate. Four others were identified for agency fielding in some capacity.

U.S. European Command is the host combatant commander for 2006 and 2007. USNORTHCOM continues as the lead for HLS/HLD CWID operations.

1997-1998

U.S. NAVY & U.S. ATLANTIC COMMAND

- ■ COMPASS deployed to nine combatant commands
- ■ Increased Compression Engine (ICE) deployed to nine combatant commands
- ■ Radiant Mercury Imagery Guard (RMIG) worldwide DoD imagery guard standard Battle Group Area Network (BGAN) fielded on six U.S. Navy ships
- ■ Combined Communications Electronics Board (CCEB) nations invited to participate in response to Joint Vision 2010 (Australia, Canada, New Zealand, United Kingdom)

1996

U.S. ARMY & U.S. CENTRAL COMMAND

- ■ Joint Total Asset Visibility (JTAV) deployed to Bosnia-Herzegovina for SFOR operations
- ■ Common Operational Modeling, Planning and Simulation Strategy (COMPASS)
- ■ Global Command and Control System (GCCS) COP validation

1995

U.S. MARINE CORPS & U.S. PACIFIC COMMAND

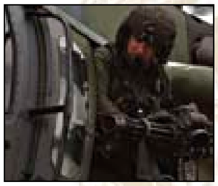
- ■ Collaborative Contingency Targeting deployed to Bosnia-Herzegovina for Stabilization Force (SFOR) operations
- ■ Contingency Theater Automated Planning System (CTAPS) fielded with U.S. Air Force
- ■ Global Broadcasting System (GBS) deployed to Bosnia-Herzegovina for SFOR operations
- ■ Theater Deployable Communications
- ■ MLS Server, U.S. Atlantic Command (USACOM, now U.S. Joint Forces Command, USJFCOM)

JWID 1994

U.S. AIR FORCE & U.S. ATLANTIC COMMAND

- ■ Common Operational Picture (COP) deployed for Operation Uphold Democracy, Haiti
- ■ All Source Analysis System (ASAS)
- ■ Tactical Packet Networks (TPN)
- ■ Network Encryption Systems (NES)
- ■ Asynchronous Transfer Mode (ATM) switches and routers
- ■ Multi-Level Security (MLS) Server, U.S. Pacific Command (USPACOM)

* THEN AND NOW is a historical compilation of technologies that have been put into operational use. For more information, contact the CWID Public Relations office: CWIDPA@langley.af.mil



CWID 2006 OBJECTIVES

Objectives Link Mission to Task

The CWID 2006 Objectives contain several key differences from those associated with past Joint Warrior and Coalition Interoperability Demonstrations.

First, the number of objectives has been reduced to narrow the focus of the annual event and to reflect a recurring theme of "Coalition Information Sharing." Second, each objective is supported by "sub-objectives" that reference clearly defined U.S. Combatant Commander and Coalition capability gaps. Finally, each "sub-objective" is related to the Universal Joint Task List (UJTL) to highlight a stronger relationship with warfighter requirements through a more defined mission-to-task linkage. These process improvements facilitate post-CWID execution efforts to develop strategies aimed at responsibly bringing solutions to warfighters.

The number of objectives has been reduced to narrow the focus of the annual event and to reflect a recurring theme of "Coalition Information Sharing."

■

Each objective is supported by "sub-objectives" that reference clearly defined U.S. Combatant Commander and Coalition capability gaps.

■

Each sub-objective is related to the Universal Joint Task List (UJTL) to highlight a stronger relationship with warfighter requirements.

OBJECTIVE

COALITION COMMAND AND CONTROL (C2)

■ Enhance the Commander's Coalition C2 capability through secure, scalable and bandwidth sensitive technologies, within and between communities of interest (COIs) and information domains of differing security classifications.

- Create a cohesive C2 relationship with and between military, coalition and non-military activities
- Improve open and secure mobile C2 capabilities between COIs
- Streamline operational decision-making for GWOT contingencies

EXPLANATION: Coalition operations require an information environment that spans multiple COIs. These COIs may be mobile, fixed or remotely located where the combination of military and/or civil agencies is likely to be affected by limited bandwidth. Within any COI, mission success relates to the commander's C2 ability to communicate directly with individual users who may be detached from fixed information domains. Decision makers and/or first responders require interoperable, reliable and/or secure wireless capabilities to receive and transmit critical voice, data, and video information to support the Network Centric warfare construct.

OBJECTIVE

COALITION INFORMATION SHARING

■ Provide solutions that improve the Commander's ability to share information within a multi-lingual coalition that is secure, scalable and bandwidth sensitive. Included in this objective are improvements to language translation tools that provide grammatically correct, militarily appropriate context, multi-language translations to support verbal and textual collaboration within and between disparate information domains.

- Multi-level and multi-domain security
- Improve utility, accuracy and language capacity of translation tools (French, Spanish, Italian, Arabic and Russian)
    1. Written-to-voice, visa versa
    2. Voice-to-voice
    3. User friendly displays

EXPLANATION: Coalition information sharing is more than providing a common operational picture at the strategic or major echelon level of command. It must be secure, scaleable in scope and functional within the theater bandwidth available at all levels of warfare. Trial proposals should be capable of using existing interface standards and protocols that define the format, content, and exchange mechanisms for shared data. Solutions must support each nation's disclosure and release policies as well as provide a secure means of consistently communicating accurate information in a multi-lingual military and/or local authority context. Possible information to exchange includes: directive commentary, friendly and hostile order of battle, targeting information, safe areas for marshalling, weather data, imagery, Global Information Services (GIS) map data, equipment status, personnel movements and other intelligence related products.

OBJECTIVE
INTEGRATED LOGISTICS

- Provide solutions for responsive, effective logistics within and between multiple information communities of interest (COIs).
  - Develop the ability to assess and display information on the movement, location and status of US and coalition partners' equipment and personnel en-route and/or deployed
  - Improve logistics data access, fusion and integration among COIs

EXPLANATION: Within the information environment of coalition, military and non-military operations, the commander must have responsive and effective logistics. Logistic data is contained within diverse logistics information systems maintained by the military and civilian agencies across the coalition. Access to that data implies combining total asset visibility and information during the transit of friendly forces into a single information presentation available across multiple information COIs. Solutions should address the locating and fusion of logistics information feeds as part of the commander's general situation awareness.

OBJECTIVE
CONTINUITY OF OPERATIONS

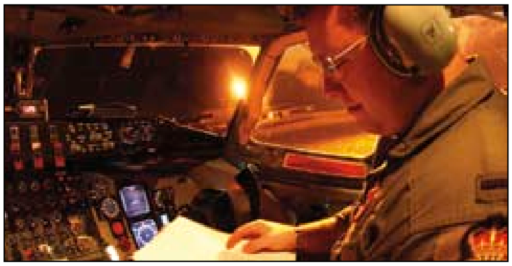
- Provide C2 solutions that enhance the Commander's ability to plan, communicate and affect coalition operations while remotely deployed. Inherent in this objective is the ability of the commander to maintain situational awareness and connectivity with subordinate activities while en route to the theater in crisis.
  - Enhance Commander's ability to rapidly deploy a joint force headquarters

EXPLANATION: Commanders are challenged to sustain their situational awareness once they depart on their assigned mission. Trial proposals must be capable of using existing interface standards and protocols that define the format, content, and exchange mechanisms for shared data. Possible information requirements include: friendly and hostile order of battle, targeting information, safe areas for marshalling, weather data, imagery, Global Information Services (GIS) map data, equipment status, personnel movements and other intelligence-related information. When appropriate, the solution must be scaleable to provide GIS and Global Command and Control System (GCCS) situational awareness information to non-military, federal, state and local participants via a protected, multi-lingual and secure network, common to all. Information exchange should support pre-event and en route planning as well as the situational awareness during the execution of operations. At a higher level, this objective involves effective information dissemination and knowledge management. This includes problems of integration, or conversion of data from one format to another, identification of producers and/or consumers of information, and how to transmit the information securely from end-to-end while supporting national disclosure/release policy.

OBJECTIVE
NET CENTRIC ENTERPRISE SERVICES

- Provide solutions that enhance the Commander's ability to collaborate and disseminate information among communities of interest (COIs) in a Net Centric environment.
  - Improve information assurance
  - Improve horizontal data access, fusion and integration
  - Improve vertical and horizontal information distribution

EXPLANATION: Network Centric Enterprise Services imply that coalition, military and non-military civilian authorities can harness the power of their respective information environments to collaboratively plan and execute operations even in a bandwidth-constrained environment. Collaborative planning and dissemination of products in a bandwidth constrained environment horizontally across and vertically within COIs is an emerging issue for the warfighter, particularly as software and procedure tools become sufficiently robust to be extended from the operational to the tactical level of warfare. Operations require an information environment that is not only scaleable, but one that spans multiple COIs. These COIs may be populated and maintained by military or civil agencies or a combination of both and it is likely they will be bandwidth-constrained. The information exchange between these COIs must be accomplished in such a way that it inspires confidence at each activity that the information is being disseminated securely, and will only be available to the agreed upon and authorized participants.



LEAD COMMANDER

U.S. European Command

U.S. European Command (USEUCOM) is the unified combatant command charged with defending and advancing U.S. national interests in a 91-country area of responsibility spanning from the North Atlantic, across Europe and Russia to South Africa. Diverse is the word which best describes USEUCOM's theater, which includes many of the world's richest and poorest nations. The command maintains ready forces to conduct the full range of operations, unilaterally or in concert with coalition partners, to promote regional stability, counter terrorism and enhance transatlantic security through support of NATO.

USEUCOM is transforming its base and force structure to become more agile, expeditionary, capable and interoperable – all essential to meeting the challenges of today's complex security environment. The command strategy emphasizes preventive, "Phase 0" theater security cooperation. This approach seeks partnerships to enhance regional security capabilities in developing nations, denies safe haven for terrorists and deals today with underlying causes of conflict. Building on the strength of a transformed NATO alliance and working with key countries and regional organizations in Africa, Eastern Europe and the Caucasus are key elements of this strategy.

Equally important is establishing command and control structures and processes that take advantage of new technologies, leverage the capabilities of the Interagency Community, and enable faster, flexible planning and execution with effects-based solutions. Coalition interoperability is absolutely critical to rapidly respond to events that may occur with little or no warning. This year's Coalition Warrior Interoperability Demonstration will help us close the gaps by evaluating trial technologies that can be fielded rapidly.

USEUCOM is proud to be host combatant command for CWID 2006 and 2007.

2007 Objectives

OBJECTIVE 1

CROSS-DOMAIN DATA SHARING

■ Provide the capability to share information across multiple networks of potentially different security classifications and caveats. Emphasis should be on passing information to U.S.-controlled, coalition networks such as U.S. Central Command's Combined Enterprise Regional Information Exchange Systems (CENTRIXS) network and coalition/alliance controlled networks such as NATO's Initial Data Transfer System (NIDTS), NATO Mission Wide Area Network (WAN), or Releasable to Republic of Korea (RELROK). Data sharing encompasses the need for cross-domain solutions (CDS) and the assurance that information passed through CDS can be utilized by systems within all security enclaves. The criteria used to determine whether data can be shared should also focus on existing doctrine and/or policy-based information management and implement robust information assurance capabilities to protect data. The Global War on Terrorism (GWOT) requires CDS devices to permit collaboration with first responders, Non-Governmental Organizations (NGOs), state and local governments as well as coalition information sharing.

OBJECTIVE 2

INTEGRATED INTELLIGENCE

■ Provide solutions that improve the commander's ability to share intelligence information products (documents, images, databases, etc.) with coalition partners, including joint and coalition forces, government agencies, NGOs and first responders.

OBJECTIVE 3

INTEGRATED OPERATIONS

■ Enhance the commander's capability to command, control and coordinate across joint & coalition forces, government agencies, NGOs, and first responders.

OBJECTIVE 4

INTEGRATED LOGISTICS

■ Demonstrate the ability to access and consolidate logistical information across organizational boundaries to provide the ability to assess and display, in near real time, information on the movement, location and status of joint forces, military services, interagency, coalition, NGO and first responder equipment, supplies and personnel en route, and/or deployed.

OBJECTIVE 5

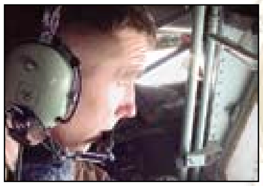
INTEGRATED PLANNING

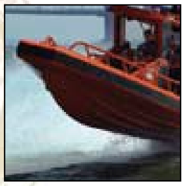
■ Provide solutions that improve the Combatant Commander's ability to conduct collaborative planning with coalition partners, including joint and coalition forces, government agencies, NGOs and first responders. Focus on enhanced collaboration and engendering a "need to share" vice a "need to know" culture.

OBJECTIVE 6

INTEGRATED COMMUNICATIONS

■ Allied and coalition partners and other-bandwidth disadvantaged users often find themselves on the frontlines, increasing risks without a robust, joint and combined, interoperable and multi-lingual information sharing capability.





NORTH AMERICAN DEFENSE - U.S. NORTHERN COMMAND

Homeland Security/Homeland Defense Commander

As a result of the events of Sept. 11, 2001, the President established a regional combatant command to ensure military defense of the homeland and to coordinate Total Force efforts toward that end.

For the first time since George Washington and the Contintental Army, the United States has a military command that focuses solely on homeland defense and support to homeland security. U.S. Northern Command's (USNORTHCOM) challenge is to harness the many capabilities and skills of the Total Force to complement those of the various federal, state, tribal, and local governments and agencies, as well as the commercial and private sector, into one coherent defensive effort.

USNORTHCOM will work with its key interagency partners to identify new ways to do business that improve cooperation, coordination and information sharing. New technologies will be embraced and harnessed to support the command's common purpose.

CONTACTS

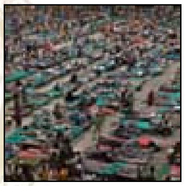
Mr. Chris Lambert
HLS/HLD Program Manager
719-554-8064
DSN 692-8064

Ms. Marie Miller
Site Manager
719-554-2802
DSN 692-2802

U.S. NORTHERN COMMAND
Area of Responsibility
U.S. PACIFIC COMMAND
Area of Responsibility
U.S. SOUTHERN COMMAND
Area of Responsibility

PRIMARY MISSION

Deter attacks against the United States, its territories, possessions and bases and employ appropriate force should deterrence fail.



DEPARTMENT OF HOMELAND SECURITY
FEDERAL EMERGENCY MANAGEMENT AGENCY

Lead Federal Agency

FEMA protects our nation's citizens and institutions from all types of hazards through a comprehensive, risk-based emergency management program of preparedness, prevention, response, and recovery. DHS/FEMA is responsible for leading the nation's effort of response and recovery for federally declared natural catastrophes, as well as incidents involving nuclear, biological, chemical or explosive material on U.S. soil. During a federally declared disaster, DHS/FEMA coordinates mission assignments for more than 25 other federal agencies and departments, including the Department of Defense.

FEMA will again support and participate in Coalition Warrior Interoperability Demonstration (CWID) 2006 as one of the lead federal agencies to U.S. Northern Command (USNORTHCOM) and its mission of Homeland Defense and Military and Assistance to Civil Authorities (MACA).

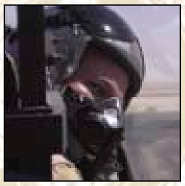
Building the nation's capability to rapidly and effectively respond to disasters of all kinds will require a strong commitment to standard setting. Standards are critical in key areas. For example, in too many instances—including response to the World Trade Center attacks—first responders and government officials were not able to fully communicate because of differing communication standards. Also, mutual aid was hindered by incompatible equipment. Baseline standards must be in place at the state, territory, tribal, local government, and first responder level to provide an effective nationwide system of emergency management.

Baseline standards must be in place to provide an effective nationwide system of emergency management.

To improve telecommunications technology between local, state and federal responders during national crises, FEMA officials are working with CWID 2006 to enhance and secure communications in the field. DHS/ FEMA is assisting in implementing solutions for a rapid deployment of an emergency communications network strategy that includes coalition command and control; coalition information sharing; and providing solutions for responsive, effective logistics within and between communities of interest.

In recent years, the U.S. has experienced natural disasters and terrorist events. Since becoming part of DHS, FEMA's primary mission and approach to carrying it out have not changed. FEMA remains committed to an all-hazards approach to emergency management. The all-hazards philosophy recognizes that the same comprehensive framework of mitigation, preparedness, response, and recovery can be used to address the impacts of all types of disasters.

Through FEMA's participation in CWID 2006, information sharing will occur across multiple domains to enhance response and recovery efforts to any catastrophic event.



NATIONAL GUARD BUREAU

Driving a Coordinated Response

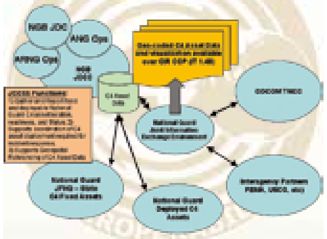
The devastating hurricane season of 2005 demonstrated the urgent need to develop, test, and exercise joint C4 solutions required to coordinate effective government response to natural and man-made disasters. The National Guard, in partnership with U.S. Northern Command (USNORTHCOM), has developed a Joint CONUS (Continental U.S.) Communications Support Environment (JCCSE) concept to address the organizational and IT capabilities required for Homeland Defense/Civilian Support (HLD/CS) mission coordination. CWID is a venue to assess operating procedures and related C4 solutions to support JCCSE development with military and civilian mission partners.

The National Guard Bureau (NGB) is managing four interoperability trials at CWID 2006 that demonstrate potential solutions to the following JCCSE information technology (IT) capability requirements:

- A Common Operational Picture (COP) encompassing all levels, and readily shared with all mission partners
- Continuous situational awareness of IT resources so they can be more effectively employed to support users at all levels, including at any incident site throughout the States & Territories
- A collaborative information exchange environment for support of inter-agency situational awareness, information sharing, and collaboration requirements, and supported by IT capabilities that are simple to deploy and use
- Deployable incident area communications support throughout the 54 States/Territories to extend collaborative information exchange capabilities to any incident site and Joint Task Force/Task Force locations

The National Guard will also test procedures related to collaborative command and control and mission coordination within the National Guard and among our HLD/CS mission partners.

The CWID domestic scenario enables the National Guard to demonstrate enhanced interoperability and information flows among command and coordination nodes at all levels of incident response: the incident area, deployed Task Forces, the JFHQ-State Joint Operations Center, and the NGB Joint Operations Center. The National Guard will leverage CWID trials to demonstrate enhanced collaboration and coordinated incident response with USNORTHCOM, U.S. Coast Guard, U.S. Navy, FEMA, and DHS operational nodes and role players at three CWID sites. The South Carolina National Guard will be supporting an enhanced incident area deployable communications demonstration and test in Charleston, S.C., through the CWID Hurricane scenario event. The Delaware National Guard will be supporting trial assessment and operations for the model State JFHQ and the National Guard Bureau (NGB) Joint Operations Centers at Naval Surface Warfare Center, Dahlgren, and USNORTHCOM CWID sites, respectively.


NGB JOC
ANG Ops
ARNG Ops
NGB JOCC
C4 Asset Data
National Guard Joint Information Exchange Environment
National Guard JFHQ - State C4 Fixed Assets
National Guard Deployed C4 Assets
Interagency Partners FEMA, USCG, etc)

JCCSE establishes inter-agency information sharing and collaboration capabilities that encompass mission partners at the National, State, and Local levels, and provides the means to extend those capabilities to any incident site.

MISSION STATEMENT

The JCCSE is an umbrella term that encompasses all of the vital organizations and supporting netcentric IT capabilities required by the National Guard to support USNORTHCOM, USPACOM, USSTRATCOM, USJFCOM, and other DoD and non-DoD partners by extending interagency and intergovernmental trusted information sharing and collaboration capabilities from the national level to the state and territory and local levels, and to any incident site throughout the United States and its territories.

CONTACT

Maj. Charles Pedigo
System Architect
charles.pedigo@ngb.army.mil

CWID will help the National Guard and its mission partners validate JCCSE organizations, procedures, and information exchange required for HLD/CS incident management and an incident response-focused common operational picture (COP). This COP should support a unified response to incidents through enhanced situational awareness of C4 and other fixed and deployable assets, as well as the assembly of operational, intelligence, logistics, and network operations information vital to conducting joint military operations in support of civilian authorities.

The NGB Joint Operations Center will be modeled at CWID to demonstrate enhanced JCCSE capabilities for State JFHQs, USNORTHCOM, as well as interagency mission partners. The NGB JOC is the primary channel of communication and coordination at the federal level for the National Guard community, and plays a pivotal coordination and information sharing role leveraging and employing National Guard resources from a regional and national perspective. The scenario events and technology assessments developed for CWID will help NGB validate operational procedures and supporting information exchange between the NGB Joint Operations Center and State JFHQs, and in relation to other command and coordination nodes.

U.S. JOINT FORCES COMMAND

CWID Oversight Command

United States Joint Forces Command (USJFCOM) has oversight responsibility for the yearly planning and execution cycles of CWID.

USJFCOM assumed oversight responsibility for the planning and execution cycle of CWID 2005 and beyond July 2004. Concurrent with that responsibility, USJFCOM established a partnership with Allied Command-Transformation (ACT) to manage CWID and resolve National, Alliance, and Coalition interoperability issues as forcing agents for change.

On behalf of the Chairman, and in coordination with the host combatant command, USJFCOM consolidates, formulates and coordinates CWID overarching objectives derived from combatant commander capability gaps, Combined Communications Electronics Board (CCEB) nations and NATO issues. Incorporation of service and coalition related challenges to CWID Objectives ensure tighter alignment of C4ISR interoperability trials and subsequent solutions.

USJFCOM chairs the Senior Management Group (SMG), the governing body for CWID. It is a standing O-6 level group responsible for planning, execution and funding allocation decisions.

The CWID event is one of USJFCOM's engines for transforming the U.S. Military. In concert with interoperability trial sponsors and industry, USJFCOM assists with coordination and development of information required to support post-execution transition decisions associated with the USJFCOM Capabilities Development process. During the CWID execution phase, interoperability trials are assessed for technical, security and warfighter attributes. Results of assessments are reviewed and integrated into a senior leadership decision brief. In coordination with the host combatant Commander, Joint Staff and SMG leadership, USJFCOM will determine an appropriate fielding vehicle to bring selected technologies to the warfighter.

COMMAND SECURITY OFFICE INFORMATION FOR HAMPTON ROADS

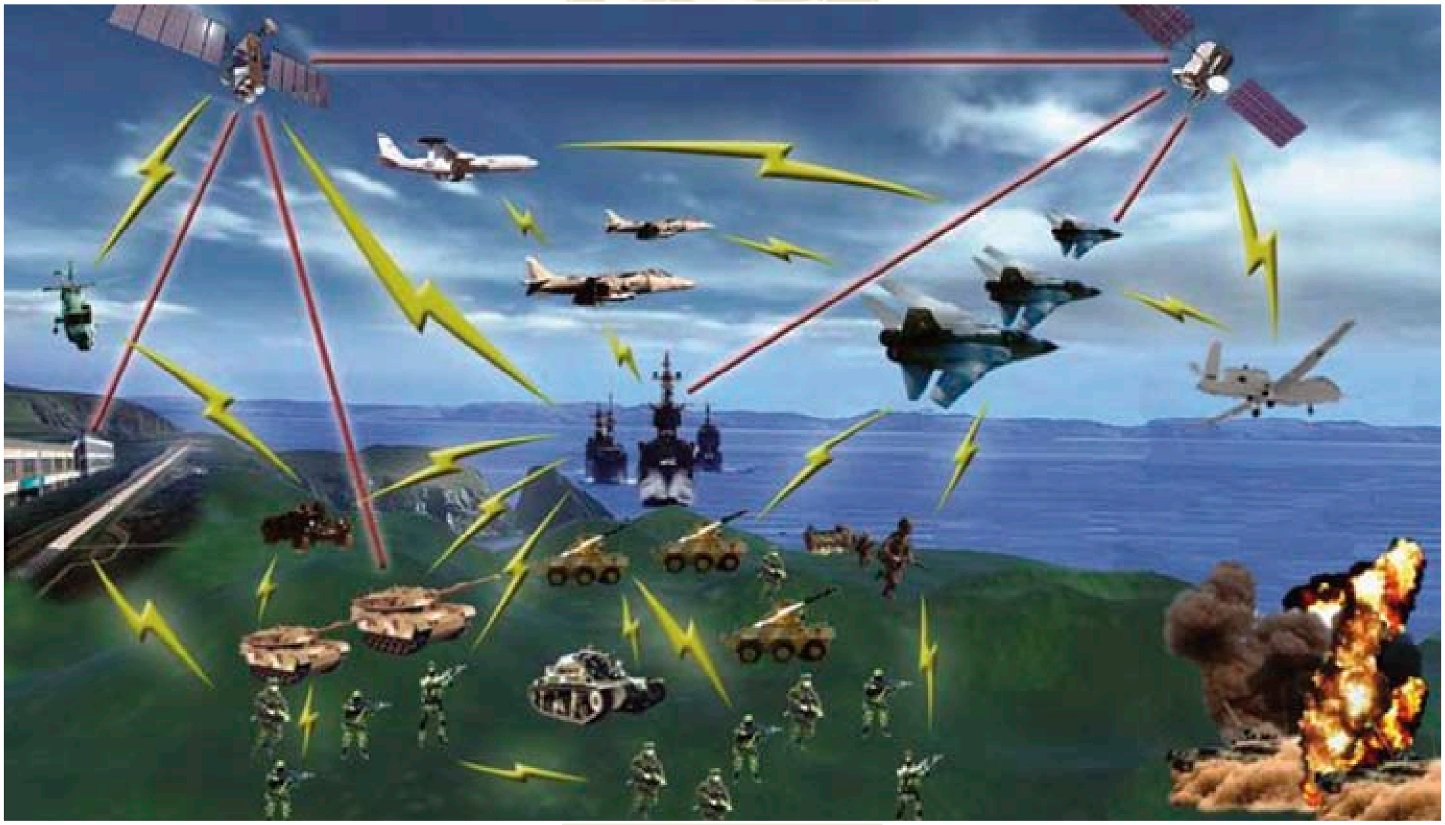
Norfolk Commander USJFCOM
1562 Mitscher Ave., Suite 200
ATTN: JOSM
Norfolk, VA 23551-2488
757.836.6405
FAX 757.836.6366

Suffolk USJFCOM
116 Lake View Parkway
Security Office
Suffolk, VA 23435-2697
757.203.7174
FAX 757.203.7512

USNORTHCOM SJFHQ-HLS
9712 Virginia Ave.
ATTN: Security Officer
Norfolk, VA 23551-2322
757.836.7453
FAX 757.836.9855

DEFENSE INFORMATION SYSTEMS AGENCY

Lead Agency, Information Technology Delivery for DoD



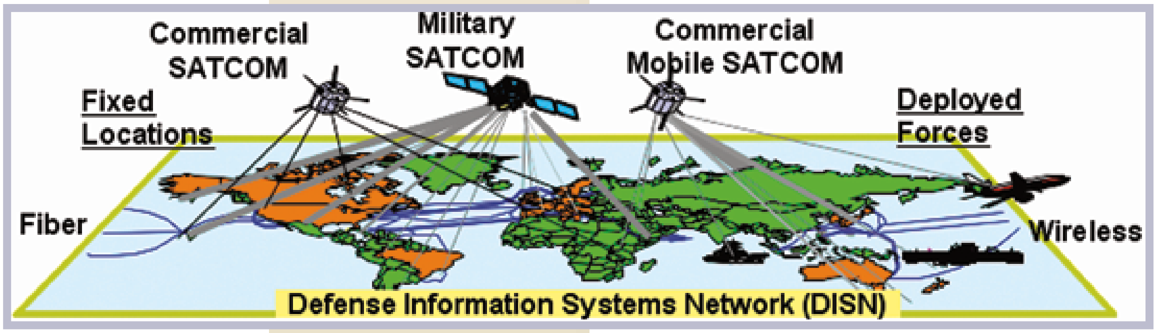
The Defense Information Systems Agency (DISA) is a combat support agency, responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, the Vice President, the Secretary of Defense, and other DoD components under all conditions of peace and war.

Providing "global net-centric solutions" means much more than superior, jointly interoperable, secure, survivable, and reliable C4 (command and control, communications, and computers) systems. DISA enables global information access and the simultaneous and synergistic employment of air, land, sea, and space warfighting capabilities.

From its Arlington, Va., headquarters and through worldwide field activities, DISA

CONTACT
Defense Information Systems
Agency (DISA)
PO Box 4502
Arlington, VA. 22204- 4502

Lt. Col. Beatriz Westmoreland
Director, CWID
Beatriz.Westmoreland@disa.mil



delivers the capability to collect and correlate data from disparate sources; collaborate with joint, coalition, intelligence, and homeland security communities; and enable them to rapidly turn decisions into strategic, operational, and tactical actions. DISA is unsurpassed in its steadfast commitment to exceeding its customers' requirements by providing solutions and enhanced capabilities that deliver measurable results. Joint cooperation is more than rhetoric at DISA – it is a philosophy and business model that we employ to deliver IT to the sharp edge of the spear.

Three specific areas in which DISA is delivering net-centric services in support of net-centric operations are: 1. Moving toward service-oriented architectures via web services and providing core enterprise services that empower the edge user to pull information from any available source. 2. Optimizing our existing, deployed communications infrastructure, the Defense Information System Network (DISN). 3. Our computing infrastructure will be the hosting facility enabling net-centric operations.

Interoperability and information-sharing are the core of successful joint and coalition operations. All partners — military Services, other government agencies, and coalition partners — must have access to systems that they can "plug into" anytime and anywhere for sharing and for discovery of data and information. These systems must work for a wide variety of missions — e.g., hurricane relief, humanitarian activities, and warfighting.

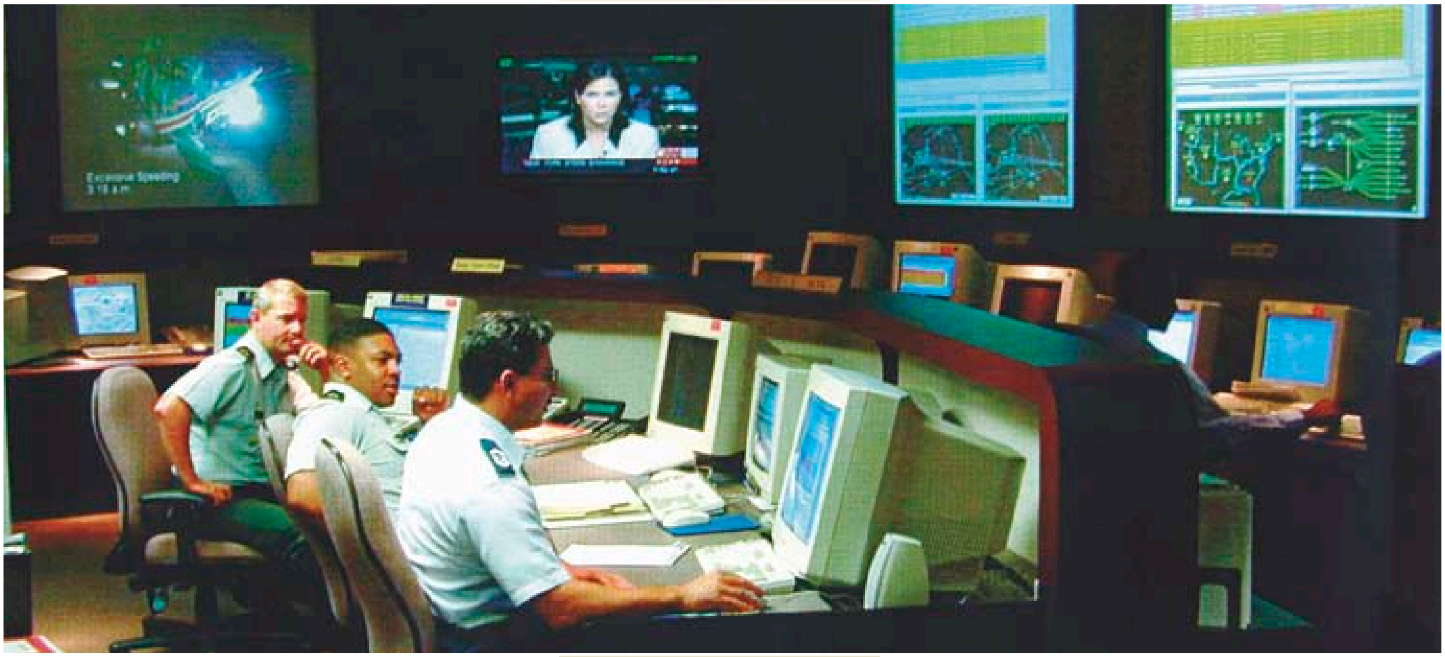
"Our challenges are to establish a standard, common network for coalition missions instead of developing new, unique networks for new missions and to lead the way in the cultural shift from 'need to know' to 'obligation to share."

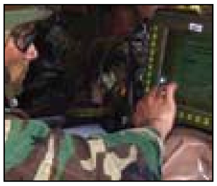
LT. GEN. CHARLES CROOM JR.
DISA DIRECTOR

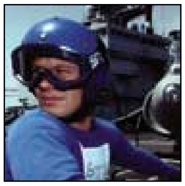
"Our challenges are to establish a standard, common network for coalition missions instead of developing new, unique networks for new missions and to lead the way in the cultural shift from 'need to know' to 'obligation to share," said Lt Gen Charles E. Croom Jr., DISA's director.

DISA is pleased to serve as the lead agency for CWID. CWID provides an opportunity to work together to improve interoperability and information-sharing. For example, three CWID 2005 programs were successfully deployed by the Department of Defense to support the relief efforts following Hurricane Katrina.

As part of CWID 2006, DISA's goal is to explore using an adaptive and secure coalition research-and-development network architecture, based on communities of interest, that can be easily and quickly scaled and configured to meet diverse multinational requirements associated with operating in an ever-changing coalition environment.





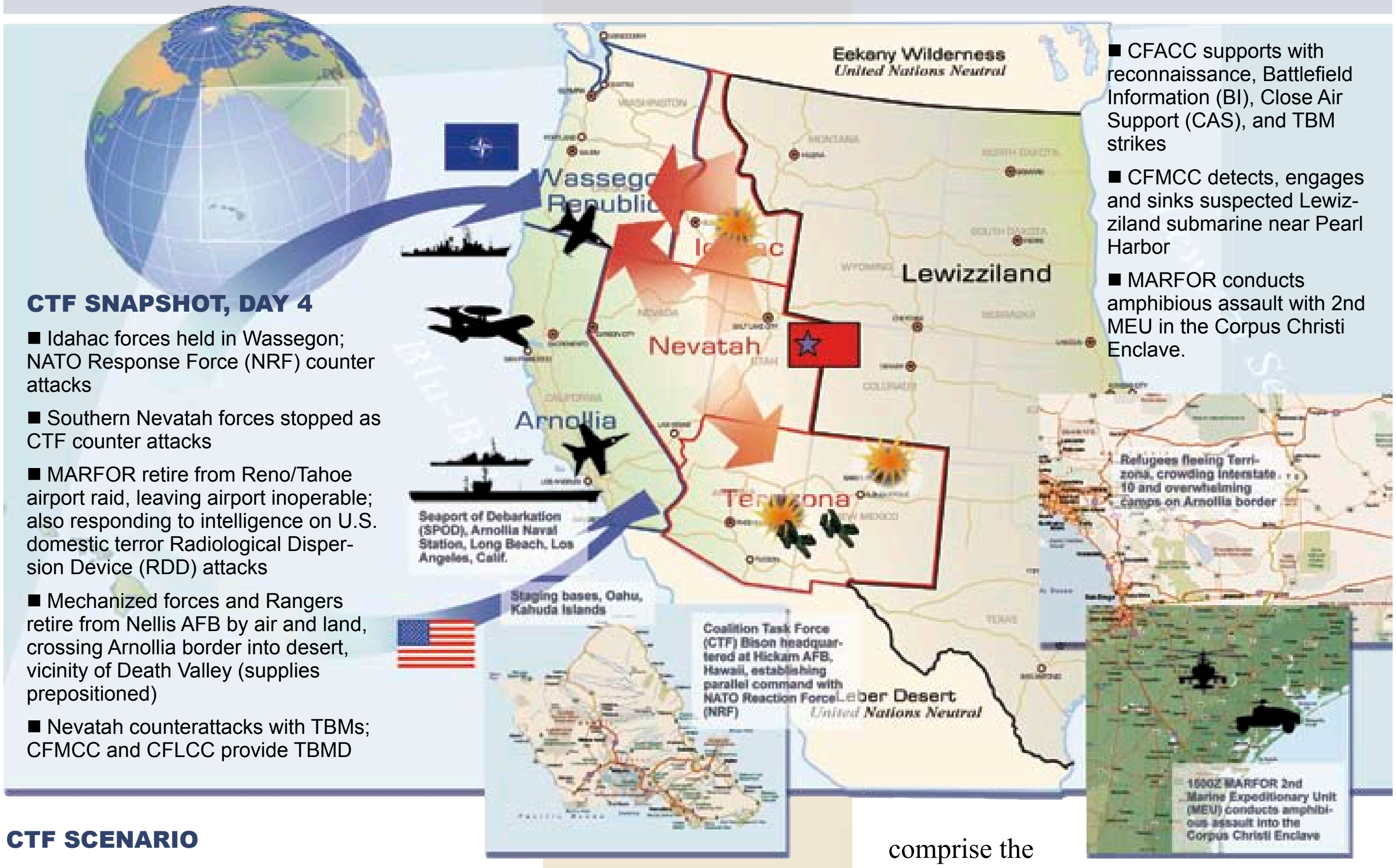


TWO-PART SCENARIO

Scripted Environment for Technology Trials

CTF SNAPSHOT, DAY 3

- ■ Nevatah-Idahac invasion of Wassegon and Terrizona imminent.
- ■ Lewizziland Carrier Task Force reinforces Blu-Blu SAG; crosses the 21 deg. latitude; maritime patrols increase; Defense Cooperation Agreement (DCA) increased for San Diego Sea Port of Debarkation (SPOD)
- ■ CTF warns Lewizziland, retire south of 21 degrees latitude; CFMCC prepares to defend Sea Line of Communications
- ■ Unknown submarine sightings off San Diego and Honolulu
- ■ CFMCC, CFLCC provide Theater Ballistic Missiles Defense (TBMD)
- ■ CFACC supports with reconnaissance, Battlefield Information (BI), Close Air Support (CAS), and TBM strikes; ensures local Analog Secure (AS) over Reno and Nellis operations
- ■ CFMCC, Marine Forces (MARFOR) preparing for amphibious landing, Corpus Christi
- ■ CFLCC, Special Operations Forces (SOF) preparing to assault Nellis
- ■ Idahac invades Wassegon; Nevatah invades Terrizona.



Seaport of Debarkation (SPOD), Arnollia Naval Station, Long Beach, Los Angeles, Calif.

Staging bases, Oahu, Kahuda Islands

Coalition Task Force (CTF) Bison headquartered at Hickam AFB, Hawaii, establishing parallel command with NATO Reaction Force (NRF)

Refugees fleeing Terrizona, crowding Interstate 10 and overwhelming camps on Arnollia border

1500Z MARFOR 2nd Marine Expeditionary Unit (MEU) conducts amphibious assault into the Corpus Christi Enclave

- ■ CFACC supports with reconnaissance, Battlefield Information (BI), Close Air Support (CAS), and TBM strikes
- ■ CFMCC detects, engages and sinks suspected Lewizziland submarine near Pearl Harbor
- ■ MARFOR conducts amphibious assault with 2nd MEU in the Corpus Christi Enclave.

CTF SNAPSHOT, DAY 4

- ■ Idahac forces held in Wassegon; NATO Response Force (NRF) counter attacks
- ■ Southern Nevatah forces stopped as CTF counter attacks
- ■ MARFOR retire from Reno/Tahoe airport raid, leaving airport inoperable; also responding to intelligence on U.S. domestic terror Radiological Dispersion Device (RDD) attacks
- ■ Mechanized forces and Rangers retire from Nellis AFB by air and land, crossing Arnollia border into desert, vicinity of Death Valley (supplies prepositioned)
- ■ Nevatah counterattacks with TBMs; CFMCC and CFLCC provide TBMD

CTF SCENARIO

U.S. European Command (USEUCOM) is the host Combatant Command for Coalition Warrior Interoperability Demonstration (CWID) 2006.

The conflict notionally occurs in Africa on the land mass and littoral of USEUCOM's area of responsibility (actually Western Continental United States). A U.S.-led Coalition Task Force (CTF) and a NATO joint force, NATO Reaction Force (NRF), comprise the friendly forces. The friendly island nation of Kahuda (actually Hawaii) has agreed to provide basing for interim staging and logistical requirements.

The CWID 2006 scenario's theme begins with a pre-existent, moderate-sized Terrizona Stabilization Force (TSF) conducting stabilization operations in one nation. Regional unrest then escalates to a regional multinational insurgency, cross-border invasion and

MAJOR EVENTS WHEN THE SCENARIO STARTS

- ■ U.S.-led Terrizona Stabilization Force (TSF) in place, Terrizona.
- ■ CTF Bison is in theater, Oahu, Kahuda Islands; forces marshaled; limited deployment into Area of Operations (southern Arnollia, Terrizona).
- ■ NRF emplaced in area of operations (Wassegon).

DISTRIBUTED TASK FORCE ELEMENTS

COALITION TASK FORCE

U.S. EUROPEAN COMMAND (USEUCOM): Combatant Command; Coalition Task Force Commander; role plays out of Kelley Barracks, Stuttgart, Germany.

CTF COALITION LAND COMPONENT COMMANDER (CFLCC): role plays out of Naval Surface Warfare Center (NSWC), Dahlgren, Va.; U.S. Army and Marine Corps elements of the CFLCC role play out of NSWC, Dahlgren, Va.

CTF COALITION FORCE MARITIME COMPONENT COMMANDER (CFMCC): role plays out of Space and Naval Warfare Systems Command (SPAWAR), San Diego, Calif.

CTF COALITION FORCE AIR COMPONENT COMMANDER (CFACC): role plays out of Electronic Systems Center, Hanscom Air Force Base, Mass.

NATO RESPONSE FORCE

Command elements of NRF role play out of Camp Jorstadmoen, Lillehammer, Norway

NATIONAL ELEMENTS

Canada, New Zealand, Australia and the United Kingdom role play units from their respective countries; Canada role plays homeland defense with U.S. Northern Command, Colorado Springs, Colo.

mid-intensity conflict. Destabilization, humanitarian crisis, and hostilities requires the deployment of coalition task forces to reinstate regional stability.

HOMELAND DEFENSE/HOMELAND SECURITY SCENARIO

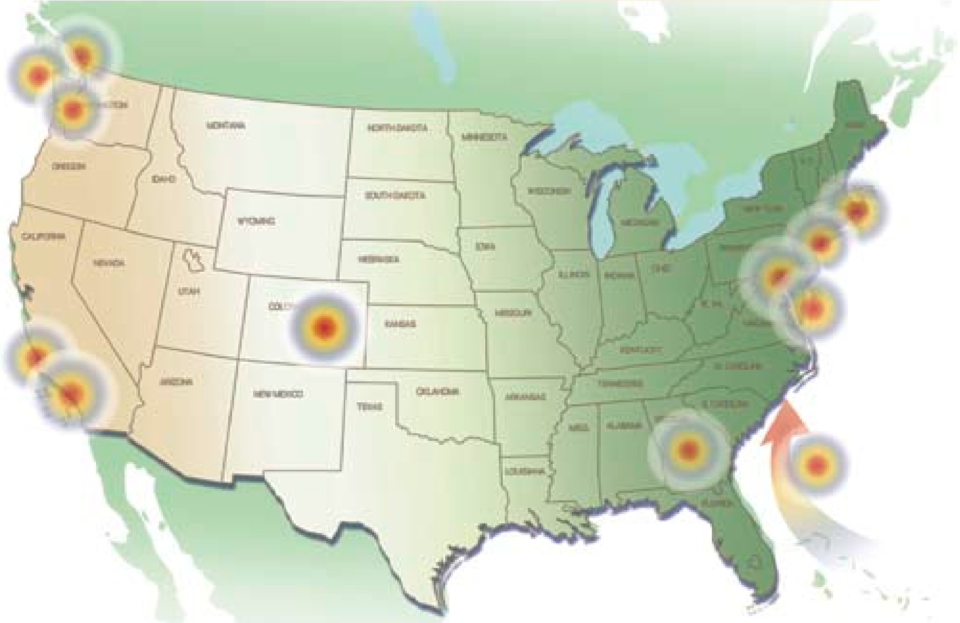
The Homeland Defense (HLD) of the United States and Canada plays out in a supporting role in this year's scenario. A serious terrorist backlash from hostilities in the notional region of the USEUCOM Theater and is directed at North America. The scenario theme includes sharing of operational and intelligence products between theaters that support each theater's mission success.

The Global War on Terrorism (GWOT) continues. Resentment toward worldwide U.S. military presence increases, particularly in the Blu-Blu Region. Terrorist groups around the world continue to forge alliances to work toward pushing the U.S. out of the Blu-Blu region.

THE HOMELAND DEFENSE MISSION

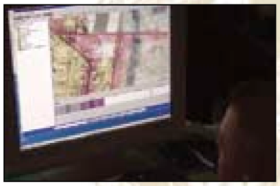
U.S. NORTHERN COMMAND (USNORTHCOM): Combatant Command; mission commander; role plays force commanders out of Colorado Springs, Colo., San Diego, Calif., and Dahlgren, Va.

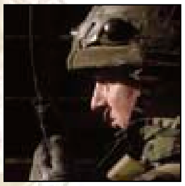
Terrorist training continues in Nevatah. Of particular concern to Homeland Security and Homeland Defense officials is the apparent intent of Nevatah to export terrorists so that they may have a direct impact on the U.S. and other Wassegon sponsors. There is evidence to suggest that a fringe group from Nevatah has split off and christened itself the "GT Brigade." Reporting suggests that the GT Brigade is attempting to coordinate its efforts with existing South American based groups and indigenous U.S. terrorist cells to execute missions on U.S. soil.



HLS/HLD SIGNIFICANT EVENTS OVERVIEW

- Chlorine rail car explosion, Quantico
- Tropical storm Anna threatens east coast
- Report of a Radiological Exposure Device (RED) vicinity of the Broadway Pier, San Diego
- Centers for Disease Control (CDC) reports possible Avian flu epidemic, Los Angeles, Boston, NYC and Vancouver
- Vehicle-Borne Improvised Explosive Devices (VBIEDs) in the Hampton Roads and Monitor Merrimac Bay Tunnels, Tidewater, Va.
- Terrorists attack tank farm, Bellingham, Wa.
- Radiological Dispersion Device (RDD) detonated in downtown Atlanta, Ga.
- Terrorists sink cruise ship, Pacific NW
- Attempted aircraft hijacking, Colorado Springs, Colo.
- Terrorist escape enroute to detainment





NETWORK ENGINEERING

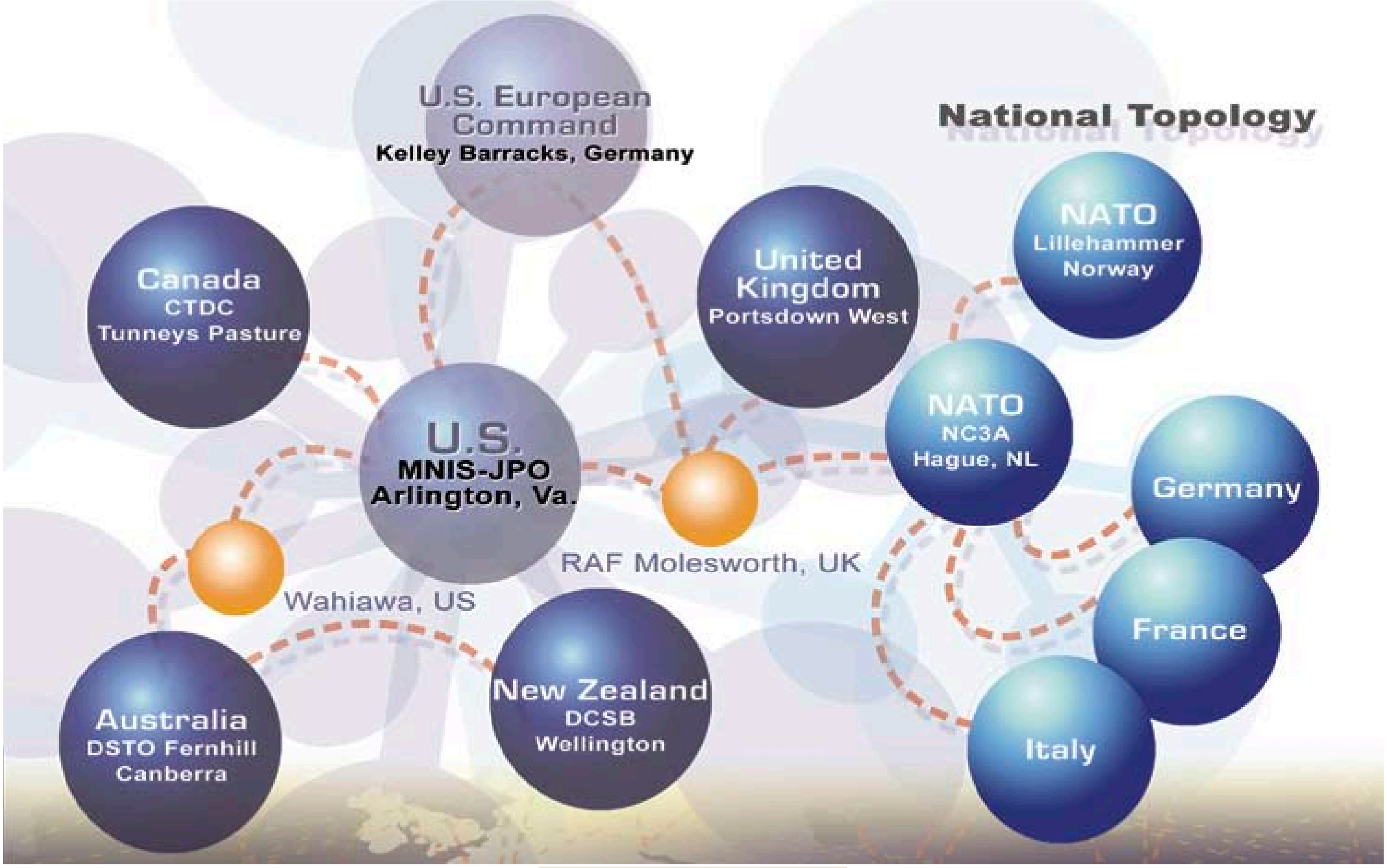
CWID, Connecting the Globe

The need for scalability and flexibility drove the development of a new classified coalition information space, called the Coalition Task Force/ NATO Reaction Force Enclave.

CWID is the Chairman's annual event to demonstrate the interoperability of cutting-edge capabilities. CWID 2006 combines the traditional CWID Warfighter scenarios with Homeland Security and Homeland Defense (HLS/HLD).

In the past, CWID utilized the Combined Federated Battle Laboratories Network (CFBLNet) Blue classified network and the DISN-LES unclassified network. Since 2005, CWID has taken a different approach. The need for scalability and flexibility drove the development of a new classified coalition information space, called the Coalition Task Force/NATO Reaction Force (CTF/NRF) Enclave. Just like the CFBLNet Blue Enclave, the CTF/NRF Enclave is a classified to the level of SECRET and protected with type-1 encryption devices. However, data on the CTF/NRF Enclave has a broader releasability than that of the Blue Enclave, allowing Partnership for Peace nations to connect to the network.

In addition to the CTF/NRF Enclave, CWID builds and uses an UNCLASSIFIED network to accommodate the interests of U.S. Northern Command (USNORTHCOM), which sponsors many trials that aim to improve Defense Support to Civil Authorities (DSCA). This enclave, known as the Homeland Defense / Homeland Security (HLS/HLD) Enclave, rep-



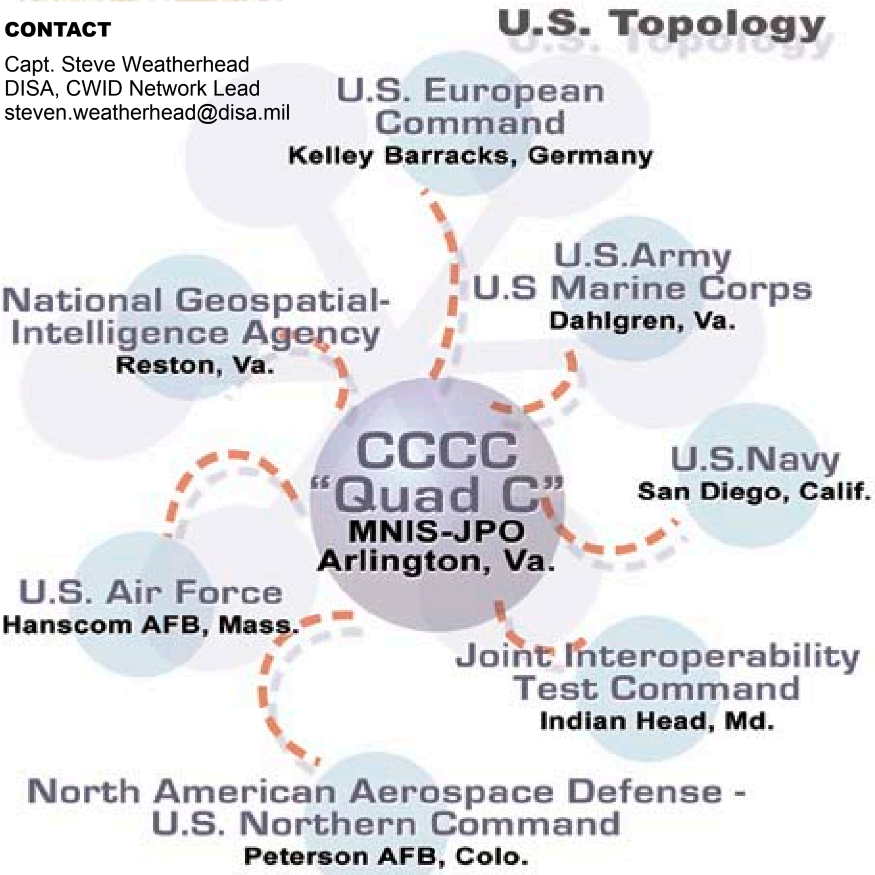
resents the network for homeland security while the warfighter enclave represents a secret network for coalition and guest nations. For the first time, Canada will join the HLS/HLD Enclave during CWID 2006 and work closely with USNORTHCOM in the testing and evaluation of DSCA technology.

The CWID networks use the DISN-LES unclassified network as the backbone with traffic separated by Type-1 encryption, supporting 30 connection sites in eight nations and NATO. The CTF/NRF Enclave, is a temporary security enclave with its own set of services, separate and unique to the CWID environment. The HLS/HLD network is built as a subset of the existing DISN-LES network architecture utilizing both existing services and those established solely for CWID 2006.

CWID 2006 involves the six perennial coalition partners: Australia, Canada, New Zealand, United Kingdom, United States, and NATO (the organization). In addition, Sweden, Finland, Germany, France and Italy are participating in the event this year.

CONTACT

Capt. Steve Weatherhead
DISA, CWID Network Lead
steven.weatherhead@disa.mil



Multinational Information Sharing Joint Program Office

The MNIS-JPO, located in Arlington, Va., directly supports and staffs the U.S. portion of the Network Operations Working Group (NOWG) and Security Working Group (SeWG) and hosts the CCCC-Rear during CWID each year. The CWID web site, assessment and MSEL servers are also hosted and maintained at the MNIS-JPO.

Support provided by the MNIS-JPO for the NOWG includes engineering and design of the network and services, provisioning of equipment and circuits, and configuration and installation of DISN-LES nodes. MNIS-JPO supports the SeWG with information assurance, network monitoring, intrusion detection, COMSEC, and certification and accreditation.

Sponsors of the MNIS-JPO include the Defense Advance Research Projects Agency (DARPA), the Defense Information Systems Agency (DISA) and the Joint Staff Director for Command, Control, Communications, and computers (JS/J6).

The MNIS-JPO facilitates rapid transfer of advanced information technology from research and experimentation stages to deployment and full-scale implementation within the Global Information Grid (GIG). The MNIS-JPO is a vehicle for implementing long-range information technology strategy and planning among DARPA, DISA and other GIG users, including coalition partners.

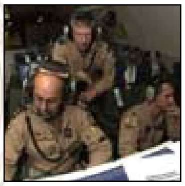
The organization also increases project coordination for the rapid insertion of advanced information technology into leading edge pilot services for joint forces and multi-service Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems and software.

The MNIS-JPO supports several Advanced Concept Technology Demonstrations (ACTD) and other information technology-related projects.

DEFENSE INFORMATION SYSTEMS AGENCY

CONTACT

Capt. Russel White
DISA MNIS-JPO
russel.white@disa.mil



ASSESSMENT

Analysts, Agencies Collect Data

The Assessment Working Group (AWG) charter is to provide the Joint Staff, Commands/Services/Agencies (C/S/A), and other interested parties with an objective assessment of qualifying Interoperability Trials (ITs) with respect to warfighter/operator utility, interoperability and Information Assurance (IA).

THE ASSESSMENT PROCESS

The ultimate goal of the assessment effort is to identify those trials that are the best candidates to provide solutions or enhancements to C4 interoperability challenges facing Joint, Coalition, Homeland Security (HLS) and Homeland Defense (HLD) operations in the near term, while protecting data and integrity on operational networks.

The AWG organization is comprised of three separate analyst teams that provide three different categories of assessments:

- Warfighter/Operator Utility
- Interoperability/Technical
- Information Assurance

These analyst teams are comprised of representatives from the CWID JMO, Joint Information and Test Command (JITC), National Security Agency (NSA) and Coalition nations. Each analyst team scrutinizes ITs, based on predefined criteria, to determine the level of assessment that can be performed. Each trial has the potential to receive any combination of the three assessment types or none at all.

The Senior Management Group (SMG) is responsible for prioritizing the participating ITs. The AWG considers this prioritized IT list, along with each specific trial's nature, varied maturity level, and the AWG's maximum assessment constraint to determine the categories of assessment for which a trial qualifies.

For trials that do not qualify for a formal assessment during CWID, the AWG coordinates with the System Engineering and Integration Working Group (SEIWG) to ensure that a summary report is provided (when applicable). This summary report documents the results of the activities performed, and the testing conducted, during CWID execution. AWG representatives highlight problem/issues and any corrective actions for each IT through observations and interviews. This information, along with first-hand warfighter/operator input collected through the JSIC Data Collection and Analysis Tool (JDCAT), and the results of their advertised data exchanges captured within the WISE Interoperability Collection and Assessment Tool (WICAT), are consolidated with the Information Assurance test results to complete the CWID assessment final report for each qualifying trial.

The ultimate goal of the assessment effort is to identify those trials that are the best candidates to provide solutions or enhancements to C4 interoperability challenges...

The final assessment report highlights IT performance with regard to meeting original stated objectives, as well as findings from the Warfighter/Operator Utility, Interoperability, and Information Assurance assessments. Following completion, the final assessment report is forwarded to the CWID JMO for inclusion in the overall

CWID Final Report. Enhanced cooperation across all U.S. and coalition assessment activities increases the validity of the assessment process and provides an opportunity to transition promising technologies identified through the CWID to the operational environment.

WARFIGHTER/OPERATOR UTILITY ASSESSMENT PROCESS

The warfighter/operator assessment focuses on "value added" to warfighters/operators, trial technical performance, and ability to meet objectives and capabilities in the CWID operational environment. During CWID execution, warfighters/operators and staff personnel operate and interact with trials, evaluating system utility by completing CWID network accessible questionnaires generated via JDCAT.

QUESTIONNAIRES ARE SPECIFICALLY DEVELOPED FOR EACH TRIAL BASED ON:

- Objectives mapped back to CWID objectives
- Predefined Master Scenario Events List (MSEL) events and/or definitive test schedules
- Trial capabilities
- Applicable Measures of Performance (MOPs) tailored to each trial

INTEROPERABILITY ASSESSMENT PROCESS

The Interoperability/ Technical assessment focuses on trial ability to exchange usable data with CWID network core/component services or other trials. Prior to execution, JITC works with each trial's staff expert to define the system interfaces that will be exercised and how these interfaces and anticipated data exchanges map to CWID objectives.

DEFINITIONS ARE DEVELOPED INTO INFORMATION EXCHANGE REQUIREMENTS (IERS):

- What information is exchanged
- Who exchanges the information
- Why the information is necessary
- How the exchanges take place.

During execution, the Interoperability Assessment team observes predetermined exchanges, ensuring that data transferred is received and processed correctly by the receiving system. Results are documented in the WICAT database developed by JITC. All information collected by JITC can be applied to the formal U.S. interoperability certification process, leading to faster fielding of technologies.

The Assessment Working Group is comprised of thee separate analyst teams that provide three different categories of assessments:

■

Warfighter/Operator Utility

■

Interoperability/ Technical

■

Information Assurance

SECURITY ASSESSMENT PROCESS

Security assessment focuses on how a trial counters identified threats and enforces identified policies consistent with appropriate usage assumptions for the projected warfighting environment.

SECURITY ENVIRONMENT ELEMENTS:

- Threats
- Assumptions
- Policies

These three are elements which a system or product might affect within that environment. Each assessed trial is documented for how well it counters environmental threats and enforces the environmental policies consistent with the assumptions for how the capability is intended for use.

Threats and policies that are adequately addressed by the capabilities of the trial are identified as "security coverage." Threats and policies not adequately addressed by the trial are a "security exposure." Security exposures that cannot be addressed by other elements represent "residual risks" that must be managed for a successful deployment.

THE SECURITY ASSESSMENT PROCESS CONTAINS THREE MAJOR PHASES

- The first phase occurs throughout the planning process and results in the documentation of functional flow, threats, and mitigation activities for each trial
- Phase two consists of basic security tests performed during CWID execution to confirm the proper implementation of the mitigation activities
- In the final phase, selected Information Assurance related trials receive assistance in developing documentation to facilitate a formal evaluation through a Common Criteria Testing Laboratory

TRIAL MATRIX

Cross Reference Trials to Sites

CWID trials for 2006 are listed in trial number order below, cross referenced to sites where they can be observed during the demonstration 12 to 21 June. For short descriptions of each trial, go to the TRIALS tab. Refer to the trials contents page at the beginning of the section to locate particular summaries.

OBJECTIVES KEY

1. COALITION C2 ■
2. COALITION INFORMATION SHARING ■
3. INTEGRATED LOGISTICS ■
4. CONTINUITY OF OPERATIONS ■
5. NET-CENTRIC ENTERPRISE SERVICES ■

TRIAL NO.	SYSTEM TITLE	EUCOM	NORTHCOM	DAHLGREN	SPAWAR	HANSCOM	AUSTRALIA	CANADA	NEW ZEALAND	UNITED KINGDOM	NATO	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	OBJECTIVE/S ADDRESSED
IT01.01	Northern European Command - C2 Information System (NEC CCIS)					■			■	■		Denmark	NATO, Denmark	**5**, 1, 4
IT01.14	U.S. Chemical Biological Radiological and Nuclear Modeling (USCBRNM)			■					■	■		Joint Project Manager Information Systems (JPM IS); UK Defense Science & Technology Laboratories (Dstl), International Task Force 49	JPM IS, Dstl International Task Force 49	**1**
IT01.15	C4I Defense	■		■	■	■				■	■	Italy	C3I Consortium, SELEX-SI SpA	**1**, 4
IT01.20	Integrated Information Management System			■	■		■					US Air Force	US Army, AFRL	**1**, 5
IT01.28	Mission Management Suite (MMS)					■	■	■			■	Canada	Canadian Air Force, ATESS Trenton	**1**
IT01.34	Mobile / Static Real-Time Radiological Surveillance Network (MobRadNet)		■	■	■			■				Canada	Dr. Robert McFadden	**1**
IT01.39	FIRST Responder INTERoperable COMMunications (First Inter-Comm™)		■									USNORTHCOM	BAE Systems	**1**
IT01.48	Emergency Response Coalition - Common Operating Picture		■	■								National Guard Bureau	National Guard Bureau	**1**
IT01.50	Multinational Interoperability Toolkit (MIT)	■			■		■			■		US Navy	SPAWAR	**1**
IT01.53	Coalition and Civil Agency Capable Wireless Information Transfer System (C3WITS)	■	■	■	■				■			US Navy	General Dynamics C4 Systems	**1**, 3
IT01.54	Coast Guard C2 (Deepwater COP) (CG-C2)		■	■	■							US Coast Guard	Lockheed Martin Corporation	**1**
IT01.62	MobileForcesSolution (MOFS / MCCIS)			■	■				■			Germany	German Navy, T-Systems Enterprise Services GmbH	**1**, 4, 5
IT01.63	IPC Information Systems, LLC Multimedia Command and Control Solution (MCCS)		■	■								FEMA	IPC Command Systems	**1**
IT02.21	The Multi National Coalition Security System (MNCSS)			■	■	■	■	■	■	■		Canada	Titus Labs, Microsoft Corp.	**2**, 5
IT02.24	M3Data Information Sharing System (M3Data ISS)							■		■		Canada	ARTIS	**1**
IT02.25	Distributed Common Ground System (DCGS)			■	■	■		■		■		US Air Force	Raytheon Intelligence and Information Systems	**2**

OBJECTIVES KEY

1. COALITION C2 ■
2. COALITION INFORMATION SHARING ■
3. INTEGRATED LOGISTICS ■
4. CONTINUITY OF OPERATIONS ■
5. NET-CENTRIC ENTERPRISE SERVICES ■

TRIAL NO.	SYSTEM TITLE	EUCOM	NORTHCOM	DAHLGREN	SPAWAR	HANSCOM	AUSTRALIA	CANADA	NEW ZEALAND	UNITED KINGDOM	NATO	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	OBJECTIVE/S ADDRESSED0
IT02.45	Command Center Portal Framework (CCPF)		■				■	■		■		Canada	xwave	**2**
IT03.09	Document Access Servelet (DAS)	■	■	■	■	■		■	■		■	USEUCOM	Information Security Corporation	**5**
IT03.16	Intelligent Road/Rail Information Server (IRRIS)	■	■	■	■		■			■		US Army	US Army, GeoDecisions	**3**, 5
IT04.03	Wide Area Interoperability System (WAIS) and ACU-1000		■						■			USNORTHCOM	Raytheon JPS Communications	**1**, 2
IT04.33	Logik v3.0 for Rapid Intelligence Analysis and Exploitation	■	■	■	■			■		■		Canada	Coredge Software, iFathom Corporation	**4**
IT04.36	Global Broadcast Service (GBS)		■	■					■			DISA	GBS JPO	**1**, 4, 5
IT04.46	Joint C4 Coordination Support System (JCCSS)		■	■								National Guard Bureau	National Guard Bureau	**1**
IT04.61	MCCIS-I				■						■	Italy	Italy, Canada, NATO ACT, Engineering SpA Rome	**1**
IT05.06	Visualization for Information Assurance (VIA)			■					■			US Air Force	Applied Visions, Inc.	**5**, 1, 2
IT05.13	Coalition Command Collaboration Services (CCCS)							■	■		■	Australia	Microsoft Corp.	**4**, 1
IT05.17	WMD Collaborative Advisory Response System (WMDCARS)	■	■				■					USNORTHCOM	DTRA	**1**, 5
IT05.32	Guard Net Portal (GNP)	■	■	■	■							US Navy	Tidewater Technology Group	**1**, 5
IT05.37	Joint Effects Based Command and Control (JEBC2)	■	■		■			■				USNORTHCOM	The Boeing Company	**1**, 2, 3, 5
IT05.41	Knowledge Management Framework							■				Canada	Lockheed Martin Corporation	**5**
IT05.47	HLS-HLD Collaborative Information Exchange Environment (HLS-HLD CIEE)		■	■								National Guard Bureau	National Guard Bureau	**1**
IT05.51	FORCEnet Distributed Channel Services (FnDCS)	■	■	■	■		■			■		US Navy	Lockheed Martin Corporation	**5**, 1
IT05.52	Rapid Triage Medical Workbench (RTMW)		■	■	■			■				USNORTHCOM	AMITA Corporation	**5**, 3
IT05.66	Coalition Shared Information Environment (COSINE)	■					■					NATO	NATO NC3A	**2**, 5